



# **High Technology Crime In California**

**Annual Report  
To the  
Governor and Legislature  
For  
2006**

**Submitted By  
The High Technology Crime Advisory Committee  
High Technology Theft Apprehension and Prosecution Program**

December 2006

The Honorable Arnold Schwarzenegger  
Governor of the State of California  
Sacramento, CA 95814

The Honorable Don Perata  
President Pro Tempore of the Senate  
Sacramento, CA 95814

The Honorable Fabian Nuñez  
Speaker of the Assembly  
Sacramento, CA 95814

Dear Governor, Mr. President Pro Tempore, and Mr. Speaker:

CBS News recently reported that every 79 seconds a thief hacks into a computer, steals a victim's identity, and then goes on a buying spree. The frequency of reported security breaches, while alarming, pales in comparison to the number of potential victims who have had their personal identifying information exposed. Computer/Cyber crimes and Identity Theft have cost our nation's businesses and residents more than the approximate \$3.5 billion in reported losses. Clearly, this is a BIG problem for everyone.

California led the way to combat computer crimes and Identity Theft. They began by legislating the High Technology Theft Apprehension and Prosecution Program (HTTAP). Oversight of the Program was given to the Office of Emergency Services, who seated the High Technology Crimes Advisory Committee. The Committee merged members of California corporations and law enforcement organizations to provide recommendations, strategies, and priorities for the Program. Through this Program, came ten multi-agency task forces committed to arresting and prosecuting high technology and Identity Theft offenders. The State Attorney General's Office and California District Attorney's Association sponsored laws that would protect the privacy of California citizens and bring about significant sentences for offenders and discourage those who might mimic their actions. California law led the Nation in a number of areas, including mandating public notification of significant breaches of personal identifying information. The California Department of Justice provided valuable training for the law enforcement community to investigate and prosecute high technology crimes. Finally, it was the task forces themselves who, in part, provided education to California residents about how high technology and Identity Theft crimes occur and how they can manage these risks. Joining them in this effort was the California Office of Privacy Protection.

Much was accomplished in 2006, but there is still a lot of work that needs to be done. I am very proud of what has been accomplished in the past year. Each of the participants has been committed to their tasks and their role in the Program. I especially applaud the members of the High Technology Crime Advisory Committee. Each of these participants takes time from their busy schedules and travel to the quarterly meetings, hosted in California by a selected task force. Without their invaluable input, ideas, experience, cooperation, and knowledge of their industries, such success would not be realized to date.

This report will provide you with an overview and the productivity of the High Technology Theft Apprehension and Prosecution Program, and its participating grant award recipients. It is my desire that it will provide you with the needed information to provide your constituents and bring value to all the components that make up the High Technology Theft Apprehension and Prosecution Program.

Sincerely,

William E. Eyres, Chair  
High Technology Crime Advisory Committee

Attachment

# **HIGH TECHNOLOGY CRIME IN CALIFORNIA**

## **TABLE OF CONTENTS**

	<b>Page Number</b>
Overview	1
New Laws	4
High Technology Crime Advisory Committee	7
Addressing the Problem of High Technology Crime	8
Addressing the Problem of Identity Theft	9
CDAAs Prosecution Activities	10
California Department of Justice Activities	11
Conclusion	13

### **TASK FORCE TEAMS**

Northern California Computer Crimes Task Force (NC <sup>3</sup> TF)	14
Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)	18
Rapid Enforcement Allied Computer Team (REACT)	22
Southern California High Tech Task Force (SCHTTF)	25
Computer and Technology Crime High-Tech Response Team (CATCH)	28

### **APPENDIX**

Appendix A – California Penal Code Sections 13848-13848.8	31
Appendix B – High Technology Crime Advisory Committee Roster	41
Appendix C - High Technology Crime Regional Task Forces High Tech/Identity Theft	45
Appendix D – By-Laws	49

## OVERVIEW

The California High Technology Crimes Task Force strategy was created through Senate Bill 1734 in 1998 to help combat computer-related crimes such as: network intrusions, computer hacking, theft of trade secrets, counterfeiting and piracy, telecommunications fraud, and theft of high tech related equipment and cargo. This legislation established the High Technology Theft Apprehension and Prosecution Program (HTTAP) which is funded through the Governor's Office of Emergency Services (OES).

Since 1998, the program has expanded to include five regional task force teams within the state of California and covering 30 counties. The mission of the HTTAP Program is the investigation, apprehension, and prosecution of high technology crimes.

Each of the task force teams are multi-jurisdictional and multi-agency teams; consisting of local, county, state, and federal investigators and prosecutors. Each team has the ability to cross borders which hinder local investigators. Investigators are able to pursue, arrest, and prosecute a wide range of criminal offenders, in a greater number of jurisdictions. Each can provide high technology-oriented service to the communities served by all the task forces collectively.

The HTTAP Program was expanded in 2001 to address the ever-growing problem of Identity Theft. Five additional task force teams, specializing in this area, were created to focus on combating Identity Theft in California. These Identity Theft task force teams work collaboratively with the five original HTTAP High Tech task force teams. The Identity Theft teams were modeled similarly to the High Tech task force teams, in that they too are multi-jurisdictional and multi-agency staffed. Additionally, they enjoy the partnerships of various privacy protection organizations that provide referrals and consumer protection information to the public.

Unfortunately, there are no government agencies that truly collect or track computer-related crimes. This is not for a lack of interest or appreciation for the impact of computer-related crimes to our communities, but because current efforts show merely a trend and are not a reliable source to show the actual position of computer-related crimes. This is true for three reasons; first, the fast processing speed of computers renders criminal activity extremely difficult to detect. Second, many law enforcement agencies lack the needed expertise to deal with high technology criminality. Lastly, even if the criminal activity is detected, many businesses are reluctant to contact law enforcement or make a report for fear of negative impact on their business and business relationships.



Agencies, such as the FBI, conduct Computer Crime Surveys primarily of the business community. From these surveys, we can begin to validate why pure statistics may not be the best measurement of high technology crimes. Their most recent survey (2005) provides these key findings:

- Nine of 10 organizations experienced a computer security incident, with 20% of them suffering 20 or more attacks each year.
- More than one in five organizations experienced port scans and network or data sabotage. The leaders were viruses and spyware (79.5%).
- Attacks originated from 36 different countries, with the U.S. (26.1%) and China (23.9%) accounting for more than half of the intrusion attempts (masking technologies make it difficult to get an accurate reading).
- 44% reported intrusions from within their own organizations.
- Only 9% of those surveyed said they reported incidents to law enforcement, believing the infractions were not illegal or that there was little law enforcement could or would do.
- Total losses were \$32 million, with viruses and worms accounting for \$12 million.

Further supporting these findings are the three year records of the five high tech task force teams in California. In 2006, the number of investigated cases dropped from a high of 2,097 to 1,164. Often, these drops reflect the reluctance of victims to contact law enforcement. It may also suggest greater security measures being applied by businesses and residents. Another contributing factor to such a drop is the successful prosecution of computer-related crimes. In 2006, about 479 persons were convicted in those investigated cases. This was a record number of convictions for the task forces in the past three years. Finally, more than 620 criminal cases were filed in 2006, another record, with more than \$224 million dollars in losses. This dollar loss reflects the lowest number of losses for the past three years. One of the primary goals of the task forces has been to use education in conjunction with arrests, prosecutions, and convictions to minimize the financial losses to California businesses and its citizens.

In 2006, we saw a record number of security breaches from local businesses, universities, major retailers, and database aggregate companies. Each of these breaches brought on new anxieties for California residents and a greater need to guarantee security of the personal identifying information of consumers. The number of potential victims has been astronomical, along with the mandate to provide notification and credit repair resources to actual victims.

According to the Federal Trade Commission, California has maintained their number three national ranking among reported victims. However, based on populations of 100,000 or more; Napa, Madera, Yuba City, Stockton, and Bakersfield residents found their reporting frequency in the top 25 cities in the nation. The FTC's most recent report (2006) points out that nearly 60% of Identity Theft victims do not contact a law enforcement agency and obtain a report. Yet, more than one third of all reported incidents to the FTC; claim they were victims of Identity Theft fraud. Unauthorized credit card charges were the leading contributor to the more than \$1.1 billion in losses to fraud victims. Demonstrating the critical need for a high tech component to compliment Identity Theft investigations, 60% of reporting victims were claimed by e-mail and web based contacts with the perpetrator(s).

The fraudulent use of personal identifying information of another for employment purposes accounts for about 14% of complaints to the Federal Trade Commission. Consumers in the 18-29 age set were the largest age group that reported losses from this type of fraud. Often, these are the ages of persons who are seeking their first job or permanent position. Educating the public to closely watch their credit reports and vigilantly review their credit statements, remains a goal of the Identity Theft task force teams. Clearly the public is still not taking advantage of California legislation which mandates a law enforcement agency take a report and begin an immediate investigation. Security of personal identifying information remains an educational goal for California businesses and the task forces. As striking as the enforcement efforts are by the task forces, the cooperative protection of personal data by California residents and businesses continue to be the benchmark of success.

Collectively, the Identity Theft task force teams have achieved tremendous successes over the past three years of their enforcement and education efforts. More than 21,000 members of the public and law enforcement have received training in the area of Identity Theft prevention and investigation. During this same time frame, the task force teams have averaged more than 2,050 investigations, 650 criminal filings with more than 550 convictions, and provided criminal Identity Theft protection services to an excess of 95,900 California residents.

## NEW LAWS

The following bills dealing with high technology crimes and identity theft were recently introduced. A summary and the author of each, is shown below. For details on any pending California high technology legislation, please visit the web site for the California District Attorneys' Association at [www.cdada.org](http://www.cdada.org) or send an email to High Tech Crimes Research Attorney Charles W. Barnes at [cbarnes@cdada.org](mailto:cbarnes@cdada.org).

- Title: AB 64 – Recording Crimes  
Author: Cohn (D)  
Summary: Relates to existing law which provides that a person is guilty of failure to disclose the origin of a recording or audiovisual work if he or she sells, rent, manufactures, or possesses that work for commercial advantage or private financial gain. Reduces the required number of audio recordings involved necessary to prosecute this offense as a felony.
- Title: AB 424 – Identity Theft  
Author: Calderon (D)  
Summary: Expands the definition of personal identifying information in existing law to include an equivalent form of identification. Provides that person as used in existing law includes a firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity.
- Title: AB 546 – State Computers: Prohibited Use: Obscene Matter  
Author: Garcia (R)  
Summary: Makes it unlawful for any elected state or local officer, including any state or local appointee, employee, or consultant, to knowingly use a state-owned or state-leased computer to access, view, download, or otherwise obtain obscene matter, except for specified purposes.
- Title: AB 618 – Crime  
Author: Cogdill (R)  
Summary: Provides that a law enforcement agency may request, and a bank, credit union, or savings association must then provide, surveillance photographs and video recordings of a person accessing the financial account of a crime victim via an ATM or from within the financial institution.



Title: AB 2415 – Network Security  
Author: Nunez (D)  
Summary: Relates to the Consumer Protection Against Computer Spyware Act. Requires a device that includes an integrated and enabled wireless access point for use in a small office, home office, or residential setting, and that is used in a federally unlicensed spectrum, to either include a warning advising the consumer how to protect their wireless network connection, a warning sticker or provide other protection that, among other things, requires affirmative action by the consumer prior to use of the device.

Title: AB 2886 – Crime  
Author: Frommer (D)  
Summary: Provides that every person who, with the intent to defraud, acquires or retains possession of the personal identifying information or another person, and who has previously been convicted of identity theft, or who, with the intent to defraud, acquires or retains possession of the personal identifying information of 10 or more other persons, shall be given specified punishment. Provides the knowledgeable selling, transferring or conveying of such information shall be given specified punishment.

Title: SB1128 – Sex Offender Punishment, Control and Containment Act  
Author: Alquist (D)  
Summary: Requires courts to keep all records relating to misdemeanor actions resulting in a requirement that the defendant register as a sex offender for 75 years. Requires every district attorney's office and the Department of Justice to retain records relating to a registered sex offender for 75 years after disposition of the case. Adds new crimes to the lists of crimes that require a person to register as a sex offender, including murder in the perpetuation of or attempt to commit certain sex crimes.

Title: SB 1390 – Crime Statistics  
Author: Poochigian ®  
Summary: Amends to existing law that requires the Department of Justice to present to the Governor an annual report containing the criminal statistics of the preceding calendar year. Requires such report to contain information on arrests for identity theft crimes.

Title: SB 1699 – Financial Transaction: Privacy  
Author: Bowen (D)  
Summary: Relates to financial privacy and electronically printed receipts.  
Prohibits printing more than the last 5 digits of a credit card account number or the expiration date upon any receipt retained by the person or entity and is signed by the cardholder and any receipt retained by the person signed by the cardholder because the cardholder used a personal identification number to complete the transaction.

## **HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE**

The High Technology Crime Advisory Committee was established concurrently with the HTTAP Program. The purpose of the committee is to provide strategic oversight to the program and conduct planning in response to high technology crime in California. This committee includes representatives of the following agencies/organizations:

- A designee of the California District Attorneys' Association
- A designee of the California State Sheriffs' Association
- A designee of the California Police Chiefs' Association
- A designee of the Attorney General
- A designee of the California Highway Patrol
- A designee of the High Tech Criminal Investigators' Association
- A designee of the Governor's Office of Emergency Services
- A designee of the American Electronic Association to represent California computer system manufactures
- A designee of the American Electronic Association to represent California computer software producers
- A designee of the California Cellular Carriers' Association
- A designee of the California Internet industry
- A designee of Semiconductor Equipment and Materials International
- A designee of the California Cable Television Association
- A designee of the Motion Picture Association of America
- A designee of either the California Telephone Association or the California Association of Long Distance Companies - This position shall rotate every other year between designees of the two associations
- A representative of the California banking industry
- A representative of the Office of Privacy Protection
- A representative of the Department of Finance
- A designee of the Recording Industry Association of America
- A designee of the Consumer Union

## ADDRESSING THE PROBLEM OF HIGH TECHNOLOGY CRIME

The HTTP Program, through grants from OES, currently funds five regional task forces that comprise the California High Technology Crimes Task Force to address the growing problem of high technology crime and Identity Theft. Refer to the back of this report for a geographical representation of the areas covered by each individual task force.

During the 2005-06 fiscal year, the five high technology crime task forces collectively reported the following information:

- Filed 620 cases involving high technology crimes
- Investigated 1,164 cases involving high technology crimes
- 1,835 victims were involved in the cases filed
- 479 Arrests
- 436 convictions were obtained
- \$224,689,701 in total aggregated monetary losses was suffered by the victims

A total of \$12,136,740 was collectively awarded to the five high technology crime task forces during this period. This amount includes a 25 percent match of \$606,837 provided individually by each of the task forces.

This money was allocated collectively as follows:

- |                      |             |
|----------------------|-------------|
| • Personnel          | \$8,947,461 |
| • Operating Expenses | \$2,905,393 |
| • Equipment          | \$ 283,886  |

For detailed information on statistics and funding by each individual high technology task force, please refer to each task force's section of this report.

## ADDRESSING THE PROBLEM OF IDENTITY THEFT

As stated earlier in this report, the HTTAP Program also funds five regional Identity Theft teams to combat the rapid increase of Identity Theft.

Collectively, during the 2005-06 fiscal year, the five Identity Theft teams collectively reported the following information.

- Filed 477 cases involving Identity Theft
- Investigated 1,370 cases involving Identity Theft
- 11,189 victims were involved in the cases filed
- 590 Arrests
- 419 convictions were obtained
- \$22,515,728 in total aggregated monetary loss was suffered by the victims

A total of \$3,851,470 was collectively awarded to the five Identity Theft teams during this period. This amount includes a 25 percent match of \$192,574 provided individually by each of the task forces.

- |                      |             |
|----------------------|-------------|
| • Personnel          | \$2,379,117 |
| • Operating Expenses | \$1,076,765 |
| • Equipment          | \$ 115,578  |

For detailed information on statistics and funding by each individual Identity Theft team, please refer to each task force's section of this report.

## **CALIFORNIA DISTRICT ATTORNEYS ASSOCIATION ACTIVITIES**

As part of the HTTAP Program, funds were allocated to the California District Attorney' Association (CDAA) for the development and implementation of a statewide education and training program. This program assists local prosecutors in the efficient and effective prosecution of crimes perpetrated with the use of high technology and Identity Theft.

The CDAA High Technology Theft Prosecution Education Program provides training to prosecutors, investigators, and law enforcement officers from all 58 counties in California. This training targets the successful investigation, apprehension, and prosecution of criminal organizations, networks, and groups of individuals involved in high technology and computer-based crimes. These cases involve computer-related and/or advanced technology issues, including white-collar crimes and Identity Theft.

In addition to providing training seminars, the program supports:

- Development and publication of the high technology crimes newsletter, *Firewall*, and a prosecution manual
- Development and maintenance of online resources, including a brief bank and expert witness database
- Provision of legal research services and other assistance as needed to California prosecutors and investigators

A total of \$309,283 was awarded to CDAA in furtherance of these activities.



## **CALIFORNIA DEPARTMENT OF JUSTICE (DOJ) ACTIVITIES**

DOJ is actively involved in the HTTAP Program through two separate projects:

Department of Justice – Deputy Attorney General (DAG) Identity Theft Support  
Department of Justice – Advanced Training Center

### **DOJ Deputy Attorney General – Identity Theft Support**

There are five Deputy Attorneys General (DAGs), one Special Agent and one Special Agent Supervisor assigned to support the High Technology Identity Theft Program which is administered through the Governor's Office of Emergency Services (OES). One DAG is assigned to each of the five task forces.

The DAGs also provide education and prosecution services to rural areas within California that are not currently served by the regional units. Additionally, the DAGs serve as points-of contact for California law enforcement inquiries, and facilitate out-of-state Identity Theft-related inquiries.

Funds have been allocated to DOJ to create the HTTAP-Identity Theft Support Project, which is part of the Special Crimes Unit in the Office of the Attorney General. A total of \$434,910 was awarded to DOJ in furtherance of the DAG Identity Theft Support Project.

### **DOJ Advanced Training Center**

The DOJ Advanced Training Center (ATC) has in place an interagency agreement with the Governor's Office of Emergency Services. The goals of this agreement are:

- To provide additional high technology investigation training classes to California peace officers, especially personnel assigned to the five regional task forces
- To provide advanced training in the area of computer forensics
- To provide equipment to personnel assigned to conduct computer forensic examinations.

The primary objectives are:

- To create a program that would continuously update the curriculum for teaching high technology investigation techniques and computer forensics
- To base the changes on trends in crime, law and technology

- To create a program (a series of classes) that would train an investigator from a 'basic introduction' to high technology crimes, to an advanced level of computer forensic investigations competency
- To develop the classes necessary to complete this series
- To test the students on learned skills and knowledge of computer crime investigations

**DOJ Database:**

In March of 2006, the task forces and database sub-committee collectively came before the High Technology Crime Advisory Committee and reported that the existing intelligence database had failed to provide any worthwhile results to further criminal investigations. Having placed nearly five years worth of data into the database, made a number of adjustments in design and inputted fields, consultation with the designer, and spending a considerable number of dollars, it did not seem reasonable to continue building upon the current database model. Currently we are looking some databases, which have come on-line since the passage of this legislation that may provide intelligence data and be a better fit for the high tech and Identity Theft criminal patterns.

At the present, the California Justice Regional Information Exchange System (Cal-JRIES) is being studies and tested. This system provides both an intelligence database and electronic bulletin board for various law enforcement agencies to exchange information among one another.

## CONCLUSION

High technology and the use of data storage devices or Internet access of the web are no longer privileges of the business community or the middle class of our society. One can hardly experience a single day without the advantages of technology at their fingertips or technology impacting our very existence. We start out each day in a vehicle which probably has an electronic ignition, controlled by a small computer chip. During any given day, we access our cell phones, calculators, printers, MP3's, VoIP phones, game boxes, digital cameras and recorders, surveillance equipment, flash memory cards, disc drives, laptops, computers, social networks, the Internet, e-mail and finally, we settle down to catch up on world news events (or other entertainment broadcasts) that we used TiVo to capture. Our world has been shaped by technology and often leaves us suspended in time without it. Remember the last time you experienced a power outage? What did you get done until power was restored?

According to Data Tex Engineering, computer crimes are on the rise. It is estimated that one out of every five people has been a victim of Identity Theft or some sort of computer hacking crime. Often, they do not even know they have been victimized until months later. Experts say that Identity Theft is becoming the most complex and most invasive computer crime facing the world today.

Soon, nearly everyone will be online and conducting personal and financial business on the web. It is far easier to pay bills online than to run down to the mailbox. The Internet is a vehicle for banking, applying for credit, shopping, booking hotels and vacations, making donations, and carrying out almost any kind of transaction; both legal and illegal.

Cyber space, as it stands today, gives rise to both positive and negative consequences. The longer a computer user stays online the more opportunity a hacker has to install Malware. It is likely that as technology moves forward, computer crimes investigators will need to remain current with that technology. It is also certain that criminals too will be stay abreast of advancing technology; creating new Malware or methods to advance their criminal conduct.

Education is the most important tool to combat data loss and Identity Theft.

## **Northern California Computer Crimes Task Force (NC<sup>3</sup>TF)**

Lead Agency: ***Marin County District Attorney's Office***

NC<sup>3</sup>TF is represented by the following thirteen counties:

- |              |            |
|--------------|------------|
| Contra Costa | • Shasta   |
| • Del Norte  | • Siskiyou |
| • Humboldt   | • Solano   |
| • Lake       | • Sonoma   |
| • Napa       | • Tehama   |
| • Marin      | • Trinity  |
| • Mendocino  |            |

Through a common memorandum of understanding, NC<sup>3</sup>TF is comprised of participants from the following agencies:

- |  |   |
|--|---|
| • California Department of Justice               | • San Pablo Police Department               |
| • California Department of Motor Vehicles        | • Shasta County District Attorney's Office  |
| • Concord Police Department                      | • Shasta County Sheriff's Department        |
| • Contra Costa County District Attorney's Office | • Solano County District Attorney's Office  |
| • Del Norte County District Attorney's Office    | • Sonoma County District Attorney's Office  |
| • Federal Bureau of Investigation                | • Tehama County District Attorney's Office  |
| • Humboldt County District Attorney's Office     | • Trinity County District Attorney's Office |
| • Lake County District Attorney's Office         | • United States Postal Service              |
| • Marin County District Attorney's Office        | • United States Secret Service              |
| • Marin County Sheriff's Department              | • Vacaville Police Department               |
| • Mendocino County District Attorney's Office    | • Vallejo Police Department                 |
| • Napa County District Attorney's Office         |   |
| • Napa County Sheriff's Department               |   |
| • Novato Police Department                       |   |
| • Redding Police Department                      |   |

### **NC<sup>3</sup>TF - HIGH TECHNOLOGY CRIMES**

During fiscal year 2005-06, NC<sup>3</sup>TF received \$1,941,878 in State funds for high technology crimes. NC<sup>3</sup>TF provided a 25 percent match of \$485,470. Total grant award funds to further the investigations of high technology crimes was \$2,427,348.

During the grant period, NC<sup>3</sup>TF budgeted approximately 73 percent of its high technology grant budget on personnel costs; 25 percent on operational costs; and 2 percent on equipment.

NC<sup>3</sup>TF reported the following for cases involving high technology crimes during this grant period:

- **132** cases filed
- **363** cases investigated
- **547** victims involved in the cases filed
- **61** convictions obtained
- **368** arrests
- **\$10,492,500** in total aggregate monetary loss was suffered by the victims

### **NC<sup>3</sup>TF - IDENTITY THEFT CRIMES**

During fiscal year 2005-06, NC<sup>3</sup>TF received \$560,235 in State funds for identity theft crimes.

NC<sup>3</sup>TF provided a 25 percent match of \$140,059. Total grant award funds to further the investigation of identity theft crimes was \$770,294.

During the grant period, NC<sup>3</sup>TF budgeted approximately 83 percent of its identity theft grant budget on personnel costs; 16 percent on operational costs; and 1 percent on equipment.

NC<sup>3</sup>TF reported the following on behalf of the Identity Theft team during this grant period:

- **25** cases filed
- **146** cases investigated
- **60** victims involved in the cases filed
- **8** convictions obtained
- **25** arrests
- **225,000** in total aggregate monetary loss was suffered by the victims



### **NC<sup>3</sup>TF - STEERING COMMITTEE MEMBERS**

NC<sup>3</sup>TF receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with NC<sup>3</sup>TF. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the NC<sup>3</sup>TF Steering Committee:

- Lucas Films Ltd.
- Marin County District Attorney's Office
- Napa County District Attorney's Office
- Napa County Sheriff's Office's Office
- Securest of Systems Integration Solutions
- Solano County District Attorney's Office
- Sonoma County District Attorney's Office
- Vallejo Police Department

## **Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)**

Lead Agency: ***Sacramento County Sheriff's Department***

SVHTCTF is represented by the following seven counties:

- El Dorado
- Merced
- Placer
- SacramentoSan Joaquin
- Stanislaus
- Yolo

Through a common memorandum of understanding, SVHTCTF is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Insurance
- California Department of Justice
- California Department of Motor Vehicles
- California Highway Patrol
- California State Attorney General's Office
- California State Controller's Office
- Ceres Police Department
- Davis Police Department
- El Dorado County District Attorney's Office
- El Dorado County Sheriff's Department
- Federal Bureau of Investigations
- Folsom Police Department
- Isleton Police Department
- Merced Police Department
- Merced County Sheriff's Department
- Modesto Police Department
- Placer County District Attorney's Office
- Placer County Sheriff's Department
- Sacramento County Probation Department
- Sacramento County District Attorney's Office
- Sacramento Police Department
- Sacramento County Sheriff's Department
- San Joaquin County Sheriff's Department
- Stanislaus County District Attorney's Department
- Stanislaus County Sheriff's Department
- Turlock Police Department
- United States Attorney's Office
- United States Postal Inspection Services
- United States Secret Service
- University of California, Davis Police Department
- USDA Forest Service
- Yolo County District Attorney's Office

## **SVHTCTF - HIGH TECHNOLOGY CRIMES**

During fiscal year 2005-06, SVHTCTF received \$1,941,878 in State funds for high technology crimes. SVHTCF provided a 25 percent match of \$485,470. Total grant award funds to further the investigations of high technology crimes was \$2,427,348.

During the grant period, SVHTCTF budgeted approximately 83 percent of its high technology grant budget on personnel costs; 16 percent on operational costs; and 1 percent on equipment.

SVHTCTF reported the following for cases involving high technology crimes during this grant period:

- **324** cases filed
- **328** cases investigated
- **328** victims involved in the cases filed
- **267** convictions obtained
- **33** arrests
- **\$8,723,429** in total aggregate monetary loss was suffered by the victims

## **SVHTCTF - IDENTITY THEFT CRIMES**

During fiscal year 2005-06, SVHTCTF received \$560,235 in State funds for identity theft crimes. SVHTCTF provided a 25 percent match of \$140,059. Total grant award funds to further the investigations of identity theft crimes was \$770,294.

During the grant period, SVHTCTF budgeted approximately 77 percent of its identity theft grant budget on personnel costs; 18 percent on operational costs; and 5 percent on equipment.

SVHTCTF reported the following on behalf of the Identity Theft team during this grant period:

- **250** cases filed
- **285** cases investigated
- **743** victims involved in the cases filed
- **183** convictions obtained
- **234** arrests
- **\$2,061,355** in total aggregate monetary loss was suffered by the victims

## **SVHTCTF – STEERING COMMITTEE MEMBERS**

SVHTCTF receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with SVHTCTF. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the SVHTCTF Steering Committee:

- American Network Services
- Apple Computer
- AT&T Wireless
- California Department of Insurance
- California Department of Justice
- California Department of Motor Vehicles
- California District Attorney's Association
- California Highway Patrol
- California State Controller's Office
- Ceres Police Department
- Comcast Cable
- Davis Police Department
- DHL/Airborne Express
- DirecTV
- E Trade Financial
- El Dorado County Sheriff's Department
- Federal Bureau of Investigation

- Federal Express
- Folsom Police Department
- Hewlett Packard
- Intel Corporation
- Isleton Police Department
- Merced Police Department
- Modesto Police Department
- Motion Picture Association of America (MPAA)
- NEC Electronics
- Oracle
- Placer County District Attorney's Office
- Placer County Sheriff's Department
- Recording Industry Association of America (RIAA)
- Roseville Police Department
- Sacramento County District Attorney's Office
- Sacramento Police Department
- Sacramento County Probation Department
- Sacramento County Sheriff's Department
- San Joaquin County Sheriff's Department
- SBC
- Stanislaus District Attorney's Office
- Stanislaus County Sheriff's Department
- Systems Integration Solutions
- Tuolumne County Sheriff's Department
- Turlock Police Services
- University of California, Davis Police Department
- United States Parcel Service
- United States Attorney's Office
- United States Postal Inspection
- United States Secret Service
- USDA – Forest Service
- Verizon Wireless
- Wells Fargo Bank
- Yolo County District Attorney's Office

## **Rapid Enforcement Allied Computer Team (REACT)**

Lead Agency: ***Santa Clara County District Attorney's Office***

REACT is represented by the following five counties:

- Alameda
- San Francisco
- San Mateo
- Santa Clara
- Santa Cruz

Through a common memorandum of understanding, REACT is comprised of participants from the following agencies:

- Atherton Police Department
- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Justice
- California Highway Patrol
- Federal Bureau of Investigations
- Fremont Police Department
- Hayward Police Department
- Internal Services Department
- Mountain View Police Department
- Pacifica Police Department
- San Francisco County District Attorney's Office
- San Francisco Police Department
- San Jose Police Department
- San Mateo County Probation Office
- San Mateo County Sheriff's Department
- Santa Clara County District Attorney's Office
- Santa Clara County Sheriff's Department
- Santa Cruz County Sheriff's Department
- South San Francisco Police Department



## **REACT - HIGH TECHNOLOGY CRIMES**

During fiscal year 2005-06, REACT received \$1,941,878 in State funds for high technology crimes. REACT provided a 25 percent match of \$485,470. Total grant award funds to further the investigations of high technology crimes was \$2,427,348.

During the grant period, REACT budgeted approximately 83 percent of its high technology grant budget on personnel costs and 17 percent on operational costs. No grant funds were spent on equipment.

REACT reported the following for cases involving high technology crimes during this grant period:

- **26** cases filed
- **249** cases investigated
- **292** victims involved in the cases filed
- **25** convictions obtained
- **18** arrests
- **\$163,215,860** in total aggregate monetary loss was suffered by the victims

## **REACT - IDENTITY THEFT CRIMES**

During fiscal year 2005-06, REACT received \$560,235 in State funds for identity theft crimes. REACT provided a 25 percent match of \$140,059. Total grant award funds to further the investigations of identity theft crimes was \$770,294.

During the grant period, REACT budgeted approximately 77 percent of its identity theft grant budget on personnel costs; 18 percent on operational costs; and 5 percent on equipment.

REACT reported the following on behalf of the Identity Theft team during this grant period:

- **31** cases filed
- **95** cases investigated
- **567** victims involved in the cases filed
- **27** convictions obtained
- **26** arrests
- **\$8,616,000** in total aggregate monetary loss was suffered by the victims

## **REACT – STEERING COMMITTEE MEMBERS**

REACT receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with REACT. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the REACT Steering Committee:

- Adobe Systems
- California Attorney General
- California Highway Patrol
- Cisco Systems
- Comcast
- eBay
- Federal Bureau of Investigation
- Fremont Police Department
- Hayward Police Department
- Intel
- Internal Revenue Service
- Menlo Park Police Department
- Mountain View Police Department
- Palo Alto Police Department
- Recording Industry Association of America
- San Francisco County District Attorney's Office
- San Francisco Police Department
- San Jose Police Department
- San Mateo County Sheriff's Department
- Santa Clara County District Attorney's Office
- Santa Clara County Sheriff's Department
- Santa Clara Police Department
- Santa Cruz County Sheriff's Department
- South San Francisco Police Department
- Sun Microsystems
- United States Attorney's Office
- United States Customs
- United States Department of Homeland Security

## **Southern California High Tech Task Force (SCHTTF)**

Lead Agency: ***Los Angeles County Sheriff's Department***

SCHTTF is represented by the following three counties:

- Los Angeles
- Orange
- Ventura

Through a common memorandum of understanding, SCHTTF is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Motor Vehicles
- California Department of Social Security
- California Highway Patrol
- Culver City Police Department
- Federal Bureau of Investigations
- Glendale Police Department
- Los Angeles City Attorney's Office
- Los Angeles County District Attorney's Office
- Los Angeles County Sheriff's Department
- Los Angeles Police Department
- Orange County Sheriff's Department
- Oxnard Police Department
- Simi Valley Police Department
- United States Postal Service
- United States Secret Service
- Ventura County District Attorney's Office
- Ventura County Sheriff's Department
- Ventura Police Department

## **SCHTTF - HIGH TECHNOLOGY CRIMES**

During fiscal year 2005-06, SCHTTF received \$1,941,878 in State funds for high technology crimes. SCHTTF provided a 25 percent match of \$485,470. Total grant award funds to further the investigations of high technology crimes was \$2,427,348.

During the grant period, SCHTTF budgeted approximately 67 percent of its high technology grant budget on personnel costs; 27 percent on operational costs; and 6 percent on equipment.

SCHTTF reported the following for cases involving high technology crimes during this grant period:

- **105** cases filed
- **85** cases investigated
- **598** victims involved in the cases filed
- **57** convictions obtained
- **18** arrests
- **\$41,589,765** in total aggregate monetary loss was suffered by the victims

## **SCHTTF - IDENTITY THEFT CRIMES**

During fiscal year 2005-06, SCHTTF received \$560,235 in State funds for identity theft crimes. SCHTTF provided a 25 percent match of \$140,059. Total grant award funds to further the investigations of identity theft crimes was \$770,294.

During the grant period, SCHTTF budgeted approximately 47 percent of its identity theft grant budget on personnel costs; 50 percent on operational costs; and 3 percent on equipment.

SCHTTF reported the following on behalf of the Identity Theft team during this grant period:

- **106** cases filed
- **690** cases investigated
- **9,553** victims involved in the cases filed
- **104** convictions obtained
- **193** arrests
- **\$11,419,835** in total aggregate monetary loss was suffered by the victims

## **SCHTTF - STEERING COMMITTEE MEMBERS**

SCHTTF receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with SCHTTF. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the SCHTTF Steering Committee:

### AAA

- Adelphia Communications
- American Express
- AOL Time Warner
- AT&T Broadband
- AT&T Wireless Service
- Brotby & Associates
- Buy.Com
- Cable & Wireless
- Cellnet, LLC
- Charter Communications
- Comcast Cablevision
- Criminal Justice Department – Cal State University of Los Angeles
- Earthlink
- Executive Software
- Falcon
- Federal Bureau of Investigations
- Greenwood & Associates
- IBM Corporation
- Los Angeles County District's Attorney Office
- Los Angeles County Sheriff's Department
- MACE Group
- MasterCard
- MCI Worldcom
- Microsoft
- Motion Picture Association of America
- Nextel
- NICB
- NLECTC
- Nortel Networks
- Pacific Bell
- Pacific Telesis Group
- Paradigm Services MP/Inter
- Recording Industry Association of America
- SBC
- Software Counsel of California
- Sony Corporation
- Sprint PCS
- Telegent
- TelePacific Communications
- U.S. Attorney's Office
- Visa USA
- X.Com/PayPal, Inc
- Verizon

## **COMPUTER AND TECHNOLOGY CRIME HIGH-TECH RESPONSE TEAM (CATCH)**

Lead Agency: ***San Diego County District Attorney's Office***

CATCH is represented by the following three counties:

- Imperial
- Riverside
- San Diego

Through a common memorandum of understanding, CATCH is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement (ICE)
- California Department of Justice
- California State Parole
- California Department of Motor Vehicles
- Carlsbad Police Department
- Drug Enforcement Administration (DEA)
- Federal Bureau of Investigations
- Imperial County District Attorney's Office
- Internal Revenue Service
- Naval Criminal Investigative Services (NCIS)
- Riverside County District Attorney's Office
- Riverside County Sheriff's Department
- San Diego County District Attorney's Office
- San Diego County Probation
- San Diego County Sheriff's Department
- San Diego Police Department
- Social Security Office
- United States Postal Inspector
- United States Secret Service

## **CATCH - HIGH TECHNOLOGY CRIMES**

During fiscal year 2005-06, CATCH received \$1,941,878 in State funds for high technology crimes. CATCH provided a 25 percent match of \$485,470. Total grant award funds to further the investigations of high technology crimes was \$2,427,348.

During the grant period, CATCH budgeted approximately 63 percent of its high technology grant budget on personnel costs; 34 percent on operational costs; and 2 percent on equipment.

CATCH reported the following for cases involving high technology crimes during this grant period:

- **33** cases filed
- **139** cases investigated
- **70** victims involved in the cases filed
- **26** convictions obtained
- **42** arrests
- **\$668,147** in total aggregate monetary loss was suffered by the victims

## **CATCH - IDENTITY THEFT CRIMES**

During fiscal year 2005-06, CATCH received \$560,235 in State funds for identity theft crimes. CATCH provided a 25 percent match of \$140,059. Total grant award funds to further the investigations of identity theft crimes was \$770,294.

During the grant period, CATCH budgeted approximately 48 percent of its identity theft grant budget on personnel costs; 50 percent on operational costs; and 2 percent on equipment.

CATCH report the following on behalf of the Identity Theft team during this grant period:

- **65** cases filed
- **154** cases investigated
- **266** victims involved in the cases filed
- **97** convictions obtained
- **112** arrests
- **\$193,538** in total aggregate monetary loss was suffered by the victims

## **CATCH - STEERING COMMITTEE MEMBERS**

CATCH receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with CATCH. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the CATCH Steering Committee:

- AEA
- Border Research & Technology Center
- California Attorney General
- California Department of Motor Vehicles
- California Department of Justice
- California State Parole
- Café Soft
- Carlsbad Police Department
- San Diego City Attorney's Office
- Computer Conversion
- Cox Communications
- Evident Data, Inc
- Federal Bureau of Investigations
- High Technology Crime Investigation Association
- ICE
- Imperial County
- Internal Revenue Service
- Linksys
- MedImpact Healthcare Systems, Inc
- Open Doors Software
- Peterbuilt
- Practical Security
- Riverside Adult Probation
- Riverside County Sheriff
- Qualcomm
- Ranger Online Corporation
- RCFL Forensic Lab
- Riverside County Probation
- SAIC
- SBC
- San Diego Sheriff
- San Diego County Probation
- San Diego District Attorney
- San Diego Police Department
- SDRIW
- Software Design Assoc
- Sony
- Sony Computer Entertainment
- Source 4, Inc
- SPAWAR
- Time Warner Cable
- Time Warner ISP
- U.S. Encode Corporation
- U.S. Department of Justice
- U.S. Postal Inspection
- U.S. Secret Service
- Volonet/Redwire, ISP
- Voyager Systems, Inc
- Websense



## **APPENDIX A**

### **California Penal Code Sections 13848-13848.8**

**13848** (a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

(b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

- (1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.
- (2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wire line communications networks and law enforcement dispatch systems, and the theft, interception, manipulation destruction, or unauthorized disclosure of data stored within those computers and networks.
- (3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.
- (4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.
- (5) Software piracy and other unlawful duplication of information.

- (6) Theft and resale of computer components and other high technology products produced by the high technology industry.
- (7) Remarking and counterfeiting of computer hardware and software.
- (8) Theft of trade secrets.

(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

**13848.2** (a) There is hereby established in the agency or agencies designated by the Director of finance pursuant to Section 13820 a program of financial and technical assistance for law enforcement and district attorneys' offices, designated to the High Technology Theft Apprehension and Prosecution Program. All funds appropriated to the agency or agencies designated by the Director of Finance pursuant to Section 13820 for the purposes of this chapter shall be administered and disbursed by the executive director of the office in consultation with the High Technology Crime Advisory Committee as established in Section 13848.6 and shall to the extent feasible be coordinated with federal funds and private grants or private donations that are made available for these purposes.

(b) The Executive Director of the agency or agencies designated by the Director of finance pursuant to Section 13820 is authorized to allocate and award funds to regional high technology crime programs which are established in compliance with Section 13848.4.

(c) The allocation and award of funds under this chapter shall be made on application executed by the district attorney, county sheriff, or chief of police and approved by the board of supervisors for each county that is a participant of a high technology theft apprehension and prosecution unit.

(d) In identifying program areas that will be eligible for competitive application during the 1998-99 fiscal year for federal funding pursuant to the Edward Byrne Memorial State and Local Law Enforcement Assistance Programs (Subchapter V, commencing with Section 3750, of Chapter 46 of the United States Code, the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall include, to the extent possible, an emphasis on high technology crime by selecting funding areas that would further the use of federal funds to address high technology crime and facilitate the establishment of high technology multi-jurisdictional task forces.

(e) The agency or agencies designated by the Director of finance pursuant to Section 13820 shall allocate any increase in federal funding pursuant to the Anti-Drug Abuse Act (Public Law 100-690) for the 1998-99 fiscal year to those programs described in subdivision (d).

**13848.4** (a) All funds appropriated to the agency or agencies designated by the Director of Finance pursuant to Section 13820 for the purposes of this chapter shall be deposited in the High Technology Theft Apprehension and Prosecution Program Trust Fund, which is hereby established. The funds shall be under the direction and control of the executive director. Moneys in the fund, upon appropriation by the Legislature, shall be expended to implement this chapter.

(b) Moneys in the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement and prosecutors to deter, investigate, and prosecute high technology related crimes. After deduction of the actual and necessary administrative costs referred to in subdivision (f), the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement, state police, and local prosecutors to deter, investigate, and prosecute high technology related crimes. Any funds distributed under this chapter shall be expended for the exclusive purpose of deterring, investigating, and prosecuting high technology related crimes.

(c) Up to 10 percent of the funds shall be used for developing and maintaining a statewide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies. In addition, the Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 may allocate and award up to 5 percent of the funds available to public agencies or private nonprofit organizations for the purposes of establishing statewide programs of education, training, and research for public prosecutors, investigators, and law enforcement officers relating to deterring, investigating, and prosecuting high technology related crimes. Any funds not expended in a fiscal year for these purposes shall be distributed to regional high technology theft task forces pursuant to subdivision (b).

(d) Any regional task force receiving funds under this section may elect to have the Department of Justice administer the regional task force program. The department may be reimbursed for any expenditures incurred for administering a regional task force from funds given to local law enforcement pursuant to subdivision (b).

(e) The agency or agencies designated by the Director of Finance pursuant to Section 13820 shall distribute funds in the High Technology Theft Apprehension and Prosecution Program Trust Fund to eligible agencies pursuant to

subdivision (b) in consultation with the High Technology Crime Advisory Committee established pursuant to Section 13848.6.

(f) Administration of the overall program and the evaluation and monitoring of all grants made pursuant to this chapter shall be performed by the agency or agencies designated by the Director of Finance pursuant to Section 13820, provided that funds expended for these functions shall not exceed 5 percent of the total amount made available under this chapter.

**13848.6** (a) The High Technology Crime Advisory Committee is hereby established for the purpose of formulating a comprehensive written strategy for addressing high technology crime throughout the state, with the exception of crimes that occur on state property or are committed against state employees, and to advise the agency or agencies designated by the Director of Finance pursuant to Section 13820 on the appropriate disbursement of funds to regional task forces.

(b) This strategy shall be designed to be implemented through regional task forces. In formulating that strategy, the committee shall identify various priorities for law enforcement attention, including the following goals:

- (1) To apprehend and prosecute criminal organizations, networks and groups of individuals engaged in the following activities:
  - (A) Theft of computer components and other high technology products.
  - (B) Violations of Penal Code Sections 211, 350, 351a, 459, 496, 537e, 593d, and 593e.
  - (C) Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.
  - (D) Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.
  - (E) Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.
- (2) To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless

and wire line communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

- (3) To apprehend and prosecute individuals and groups engaged in the theft of trade secrets.
- (4) To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.
- (5) (c) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall appoint the following members to the committee:
  - (1) A designee of the California District Attorneys Association
  - (2) A designee of the California State Sheriffs Association
  - (3) A designee of the California Police of Chiefs Association
  - (4) A designee of the Attorney General
  - (5) A designee of the California High Patrol
  - (6) A designee of the High Technology Crime Investigation Association
  - (7) A designee of the agency or agencies designated by the Director of Finance pursuant to Section 13820
  - (8) A designee of the American Electronic Association to represent California computer system manufacturers
  - (9) A designee of the American Electron Association to represent California computer software producers
  - (10) A designee of the California Cellular Carriers Association

- (11) A representative of the California Internet industry
- (12) A designee of the Semiconductor Equipment and Materials International
- (13) A designee of the California Cable Television Association
- (14) A designee of the Motion Picture Association of America
- (15) A designee of either the California Telephone Association  
Or  
the California Association of Competitive Telecommunication Companies. This position shall rotate every other year between designees of the two associations.
- (16) A representative of the California banking industry
- (17) A representative of the Office of Privacy Protection
- (18) A representative of the Department of Finance

(d) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall designate the Chair of the High Technology Crime Advisory Committee from the appointed members

(e) The advisory committee shall not be required to meet more than 12 times per year. The advisory committee may create subcommittees of its own membership, and each subcommittee shall meet as often as the subcommittee members find necessary. It is the intent of the Legislature that all advisory committee members shall actively participate in all advisory committee deliberations required by this chapter.

Any member who, without advance notice to the executive director and without designating an alternative representative, misses three scheduled meetings in any calendar year for any reason other than severe temporary illness or injury (as determined by the Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820) shall automatically be removed from the advisory committee. If a member wishes to send an alternative representative in his or her place, advance written notification of this substitution shall be presented to the executive director. This notification shall be required for each meeting the appointed member elects not to attend.

Members of the advisory committee shall receive no compensation for their services, but shall be reimbursed for travel and per diem expenses incurred as a result of attending meetings sponsored by the agency or agencies designated by the director of Finance pursuant to Section 13820 under this chapter.

(f) The executive director, in consultation with the High Technology Crime Advisory Committee, shall develop specific guidelines and administrative procedures for the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program, which guidelines shall include the following selection criteria:

- (1) Each regional task force that seeks funds shall submit a written application to the committee setting forth in detail the proposed use of the funds.
- (2) In order to qualify for the receipt of funds, each proposed regional task force submitting an application shall provide written evidence that the agency meets either of the following conditions:
  - (A) The regional task force devoted to the investigation and prosecution of high technology-related crimes is comprised of local law enforcement and prosecutors, and has been in existence for at least one year prior to the application date.
  - (B) At least one member of the task force has at least three years of experience in investigating or prosecuting cases of suspected high technology crime.
- (3) Each regional task force shall be identified by a name that is appropriate to the area that it serves. In order to qualify for funds, a regional task force shall be comprised of local law enforcement and prosecutors from at least two counties. At the time of funding, the proposed task force shall also have at least one investigator assigned to it from a state law enforcement agency. Each task force shall be directed by a local steering committee composed of representatives of participating agencies and members of the local high technology industry.
- (4) The California High Technology Crimes Task Force shall be comprised of each regional task force developed pursuant to this subdivision.

(5) Additional criteria that shall be considered by the advisory committee in awarding grant funds shall include, but not be limited to, the following:

- (A) The number of high technology crime cases filed in the prior year.
- (B) The number of high technology crime cases investigated in the prior year.
- (C) The number of victims involved in the cases filed.
- (D) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, or corporations, as a result of the high technology crime cases filed, and those under active investigation by that task force.

(6) Each regional task force that has been awarded funds authorized under the High Technology Theft Apprehension and Prosecution Program during the previous grant-funding cycle, upon reapplication for funds to the committee in each successive year, shall be required to submit a detailed accounting of funds received and expended in the prior year in addition to any information required by this section. The accounting shall include all of the following information:

- (A) The amount of funds received and expended.
- (B) The use to which those funds were put, including payment of salaries and expenses, purchase of equipment and supplies, and other expenditures by type.
- (C) The number of filed complaints, investigations, arrests, and convictions that resulted from the expenditure of the funds.

(g) The committee shall annually review the effectiveness of the California High Technology Crimes Task Force in deterring, investigating, and prosecuting high technology crimes and provide its findings in a report to the Legislature and the Governor. This report shall be based on information provided by the regional task forces in an annual report to the committee which shall detail the following:



(1) Facts based upon, but not limited to, the following:

- (A) The number of high technology crime cases filed in the prior year.
- (B) The number of high technology crime cases investigated in the prior year.
- (C) The number of victims involved in the cases filed.
- (D) The number of convictions obtained in the prior year.
- (E) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

(2) An account of funds received and expended in the prior year, which shall include all of the following:

- (A) The amount of funds received and expended.
- (B) The uses to which those funds were put, including payment of salaries and expenses, purchase of supplies, and other expenditures of funds.
- (C) Any other relevant information requested.

**13848.8** (a) The executive director of the agency or agencies designated by Director of finance pursuant to Section 13820 shall also appoint the following members to the High Technology Crime Advisory Committee established by Section 13848.6.

(1) A designee of the Recording Association of America

(2) A designee of the Consumers Union

(b) The High Technology Crime Advisory Committee, in formulating a comprehensive written strategy for addressing high technology crime throughout the state, shall identify, in addition to the various priorities for law enforcement attention specified in subdivision (b) of Section 13848.6, the goal of apprehending

and prosecuting criminal organizations, networks, and groups of individuals engaged in the following activities:

- (1) Violations of Sections 653h, 653s, and 635w.
- (2) The creation and distribution of pirated sound recordings or audiovisual works or the failure to disclose the origin of a recording or audiovisual work.

**Appendix B**  
**High Technology Crime Advisory Committee**  
**MEMBERSHIP ROSTER**

<b>MEMBER/ ADDRESS</b>	<b>DESIGNATION</b>
<b>William E. Eyres -Chair</b> 8831 Berta Ridge Court Prunedale, CA 93907	American Electronic Association California Computer System Manufacturers
<b>Saul Arnold</b> Corporate Counsel, Legal Services Law Department Applied Materials, Inc. 3050 Bowers Ave. M/S 2062  P.O. Box 58039 Santa Clara, CA 95054	Semiconductor Equipment and Materials International
<b>Robert Bastida</b> Director of Corporate Security - Oracle, Inc. 500 Oracle Parkway - M/S 6op1 Redwood City, CA 95065	American Electronic Association California Computer Software Producers <b>(Alternate)</b>
<b>Bill Bowyer</b> Comcast Cable 501 Guiseppe Court, Suite D Roseville, CA 95678	California Cable & Telecommunications Association
<b>Reginald Chappelle</b> California Highway Patrol 2555 First Avenue, Room 200 Sacramento, CA 95818	California Highway Patrol
<b>Adam Christianson, Sheriff</b> Stanislaus County Sheriff's Department 250 East Hackett Road Modesto, CA 95358	California State Sheriffs' Association

**High Technology Crime Advisory Committee  
MEMBERSHIP ROSTER**

<b>MEMBER/ ADDRESS</b>	<b>DESIGNATION</b>
<b>Jack Christin, Jr.</b> Trust & Safety Counsel eBay, Inc. 2145 Hamilton Avenue San Jose, CA 95125	California Internet Industry
<b>Gail Hillebrand</b> Senior Attorney 1535 Mission Street San Francisco, CA 94103	Consumer's Union
<b>Charles Lawhorn</b> Anti-Piracy Legal Affairs 10842 Noel Street, Unit 106 Los Alamitos, CA 90720	Recording Industry Association of America
<b>Lt. John McMullen</b> District Attorney – County of Santa Clara Bureau of Investigation High Technology Crime Unit 70 West Hedding Street, West Wing San Jose, CA 95110	High Tech Crime Investigation Association
<b>Joanne McNabb, Chief</b> Office of Privacy Protection 400 R Street, Suite 3080 Sacramento, CA 95814	Office of Privacy Protection
<b>Richard Lopes, Bureau Chief</b> Division of Law Enforcement Department of Justice 4949 Broadway Sacramento, CA 95820	California Attorney General's Office

**High Technology Crime Advisory Committee  
MEMBERSHIP ROSTER**

<b>MEMBER/ ADDRESS</b>	<b>DESIGNATION</b>
<b>Colleen Pedroza</b> State Information Security Officer Office of Technology Review - Oversight & Security Unit - Department of Finance 915 L Street, 6th Floor Sacramento, CA 95814	CA Department of Finance
<b>Gary Reynolds</b> Director, Financial Crime Investigations Wells Fargo Bank 420 Montgomery Street, 4th Floor San Francisco, CA 95104	California Banking Industry
<b>Mike Robinson</b> VP & Director, U.S. Anti-Piracy Operations Motion Picture Association of America, Inc. 15503 Ventura Blvd. Encino, CA 91436	Motion Picture Association of America
<b>James Sibley</b> Deputy District Attorney - Santa Clara County 70 West Hedding Street, 4th Floor San Jose, CA 95110	California District Attorneys Association
<b>Paul S. Sieracki</b> Staff Director - Sprint (Wireless Carriers of CA) Sprint - Law & External Affairs 925 L Street, Suite 345 Sacramento, CA 95814	California Cellular Carriers Association
<b>Vacancy</b>	California Police Chiefs' Association

**High Technology Crime Advisory Committee  
MEMBERSHIP ROSTER**

<b>MEMBER/ ADDRESS</b>	<b>DESIGNATION</b>
<b>Dave Walters</b> American Electronic Association Sales California Computer Software Producers Tasman Drive, SJ9-3 San Jose, CA 95134	Cisco Systems, Inc. Worldwide Channel Director, Cisco Brand Protection 170 West
<b>Vacancy</b>	California Telephone Association CA Association of Long Distance Companies

## **APPENDIX C**

### **HIGH TECH CRIME TASK FORCES FY05/06**

#### **Northern California Computer Crimes Task Force (NC3TF)**

Edward Berberian - Project Director  
Lt. Rick Nichelman - Project Manager  
455 Devlin Road, Suite 207  
Napa, CA 94558  
Website: [www.nc3tf.org](http://www.nc3tf.org)  
Phone: 707-253-4500  
Fax: 707-253-4664

#### **Sacramento Valley Hi-Tech Crimes Task Force**

Capt. Wayne Ikeuchi - Project Director  
Lt. Bob Lozito - Project Manager  
4510 Orange Grove Avenue  
Sacramento, CA 95841  
Website: [www.sachitechcops.org](http://www.sachitechcops.org)  
Phone: 916-874-3002  
Fax: 916-874-3006

#### **Rapid Enforcement Allied Computer Team (REACT)**

James Sibley - Project Director/ Project Manager  
950 South Bascom Avenue, Suite 3011  
San Jose, CA 95128  
Website: [www.reacttf.org](http://www.reacttf.org)  
Phone: 408-494-7186  
Fax: 408-287-5076

#### **Southern California High Tech Task Force (SCHTTF)**

Lt. Robert Costa - Project Director  
Sgt. Anthony Lucia - Project Manager  
9900 Norwalk Blvd, Suite 150  
Santa Fe springs, CA 90670  
Phone: 562-347-2601  
Fax: 562-946-7506

Keith Burt –  
Project Director  
Lt. Terry Jensen -  
Project Manager  
4725 Mercury Street,  
Suite 200  
San Diego, CA 92111  
Website:  
**[www.catchteam.org](http://www.catchteam.org)**  
Phone: 619-531-3660  
Fax: 858-715-2366

## **IDENTITY THEFT FY05/06**

### **Northern California Computer Crimes Task Force (NC3TF)**

Edward Berberian - Project Director  
Lt. Rick Nichelman - Project Manager  
455 Devlin Road, Suite 207  
Napa, CA 94558  
Website: **[www.nc3tf.org](http://www.nc3tf.org)**  
Phone: 707-253-4500  
Fax: 707-253-4664

### **Sacramento Valley Hi-Tech Crimes Task Force**

Capt. Wayne Ikeuchi - Project Director  
Sgt. Mike Freeworth - Project Manager  
4510 Orange Grove Avenue  
Sacramento, CA 95841  
Website: **[www.sachitechcops.org](http://www.sachitechcops.org)**  
Phone: 916-874-3000  
Fax: 916-874-3006

### **Rapid Enforcement Allied Computer Team (REACT)**

James Sibley - Project Director/ Project Manager  
Sgt. Art Martinez - Identity Theft Supervisor  
950 South Bascom Avenue, Suite 3011  
San Jose, CA 95128  
Website: **<http://reacttf.org>**  
Phone: 408-994-7186/ 650-599-7390  
Fax: 408-287-5076



**Southern California High Tech Task Force (SCHTTF)**

Lt. Ronald Williams - Project Director  
Sgt. Robert Berardi - Project Manager  
9900 Norwalk Blvd, Suite 150  
Santa Fe springs, CA 90670  
Phone: 562-347-2660

Keith Burt - Project  
Director  
Lt. Terry Jensen -  
Project Manager  
Fred Baclagan - Identity Theft Supervisor  
4725 Mercury Street,  
Suite 200  
San Diego, CA 92111  
Website:  
**[www.catchteam.org](http://www.catchteam.org)**  
Phone: 619-531-3660  
Fax: 858-715-2366

**Department of Justice - High Tech Database**

Edward Manavian, Chief - Project Director  
Tim Bobitt, Senior Special Agent in Charge - Project Manager  
4949 Broadway, Room E130  
Sacramento, CA 95820  
Phone: 916-227-4169/ 916-227-1251  
Fax: 916-227-1228

**Department of Justice - DAG ID Support**

Mark Geiger, Senior Assistant Attorney General - Project Director  
1300 I Street, room 940-20  
Sacramento, CA 95814  
Phone: 916-324-5185  
Fax: 916-322-2368

**Department of Justice - Advanced Training Center**

Gil Van Attenhoven, Special Agent in Charge - Project Director  
11181 Sun Center Drive  
Rancho Cordova, CA 95670  
Phone: 916-464-5591  
Fax: 916-464-5577  
Website: **<http://www.ag.ca.gov/atc/index.htm>**

**California District Attorneys' Association (CDAA)**

David LaBahn, Executive Director - Project Director

Kate Killeen - Project Manager

Charles Barnes,

Research Attorney

731 K Street, Suite 300

Sacramento, CA 95814

Phone: 916-443-2017

Fax: 916-443-0540

Website: **[www.cdaa.org](http://www.cdaa.org)**

# **APPENDIX D**

## **STATE OF CALIFORNIA BYLAWS, RULES AND PROCEDURES OF THE HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE**

*Adopted: June 2005*

*Revised: March 2005*

### **ARTICLE I: NAME AND AUTHORITY**

This organization, created in the State government by statutory authority, shall be known as the High Technology Crime Advisory committee – hereinafter referred to as the “Committee.”

### **ARTICLE II: MEMBERSHIP AND CHAIRPERSON SELECTION**

#### **Section 1.**

The Committee shall be composed of twenty members. The Committee membership shall include:

- (1) A designee of the California Attorney General;
- (2) A designee of the California Highway Patrol
- (3) A designee of the California Office of Emergency Services;
- (4) A representative of the California Department of Finance;
- (5) A representative of the California Office of Privacy Protection;
- (6) A designee of the California District Attorneys Association;
- (7) A designee of the California State Sheriff’s Association;
- (8) A designee of the California Police Chief’s Association;
- (9) A designee of the High Tech Criminal Investigators Association;
- (10) A designee of the American Electronic Association to represent California computer system manufacturers;
- (11) A designee of the American Electronic Association to represent California software producers;
- (12) A designee of the California Cellular Carriers Association;
- (13) A designee of the California Internet Industry;
- (14) A designee of the Semiconductor Equipment and Materials International (SEMI);
- (15) A designee of the California Cable Television Association;
- (16) A designee of the Motion Picture Association of America
- (17) A designee of either the California Telephone Association **or** the California Association of Competitive Telecommunications Companies (CALTEL). This position shall rotate every other year between designees of the two associations;
- (18) A representative of the California Banking Industry;
- (19) A designee of the Recording Industry Association of America

(20) A designee of the Consumers Union

**Section 2.**

The chairperson of the Committee shall be selected by the Executive Director of the Office of Emergency Services from among the members of the Committee [Penal Code Section 13848.6(d)].

**ARTICLE III: POWERS AND DUTIES**

**Section 1.**

The Committee is empowered to act as the advisory board of the Office of Emergency Services in accordance with the mandates of the pertinent state acts and programs. The Committee may develop and/or modify and recommend to the Office of Emergency Services a high technology plan.

**Section 2.**

The Committee may develop policy recommendations for the Governor, the Legislature, the Office of Emergency Services and the local units of government on major criminal justice issues where a high technology nexus exists. To that end, the Committee understands itself to be the primary advisory board on technology-related criminal justice issues. Its goals include:

1. Identifying current, developing and future issues involving high technology crime and criminal justice policy and procedures relevant to such issues;
2. Developing an understanding of the issues attendant to high technology crime and making conclusions that provide the foundation for recommendations to the Office of Emergency Services, the Governor and the Legislature concerning high technology crime, criminal identification, apprehension and prosecution;
3. Issuing analysis of current or pending high technology criminal justice-related legislation;
4. Assisting California's criminal justice agencies and practitioners in the effective use of resources regarding high technology crime;
5. Coordinating studies and recommendations with the Office of Emergency Services and other criminal justice agencies with a view toward isolating issues common to high technology crime and justice.

**ARTICLE IV: COMMITTEE MEETINGS**

**Section 1.**

The Committee shall meet at such intervals as necessary to carry out its duties, but no more than twelve meetings shall be held annually. Regular meetings of the Committee shall be held at least quarterly unless, in the opinion of the Committee Chair and Vice Chair, there are insufficient items of business or insufficient funds to call such quarterly or regular meetings. The Executive Secretary of the Committee shall give a minimum of ten days written advance notice to the membership of the Committee of the time and place of a regular meeting.

## **Section 2.**

Special meetings of the Committee may be called at any time by the Committee Chair. Forty-eight hours prior notice of the time and place of such special meetings shall be given by the Chair to the members, where permitted by law.

## **Section 3.**

Meetings shall be conducted in accordance with these bylaws and Robert's Rules of Order.

# **ARTICLE V: SUBCOMMITTEES AND SUBCOMMITTEE MEETINGS**

## **Section 1.**

The Committee shall have the following subcommittees:

- Strategy Subcommittee
- Bylaws Subcommittee

## **Section 2.**

The Committee may recommend the creation of such subcommittees of its own membership as it deems necessary.

## **Section 3.**

By a majority decision, the Committee may request the review of any subcommittee's decisions or activities.

## **Section 4.**

Each subcommittee of the Committee shall meet as often as the subcommittee members find to be necessary.

## **Section 5.**

All subcommittees shall be ad hoc in nature, and sit at the pleasure of the Committee Chair and a majority vote of the membership present at the time of the subcommittee creation.

# **ARTICLE VI: OFFICERS AND DUTIES**

## **Section 1.**

The officers of the Committee shall be the Chairperson (Chair) and the Vice Chairperson (Vice Chair).

## **Section 2.**

The Chairperson shall be chosen by the Executive Director of the Office of Emergency Services from among members of the Committee, and shall serve at the pleasure of the Director. The Vice Chair shall be chosen by the membership of the Committee from among members of the Committee.

## **Section 3.**

The Chair shall preside over all meetings of the Committee, and perform such additional duties as requested by the Committee and normally executed by a chairperson. The Chair shall create such standing and ad hoc committees as are deemed necessary to carry out the powers, duties and mission of the Committee. The Chair also shall appoint all members to

both standing and ad hoc committees. All such subcommittee members shall serve at the pleasure of the Chair.

#### **Section 4.**

In the absence of the Chair, the Vice Chair shall preside at meetings and perform such additional duties as are required by the Committee and necessitated by the absence of the Chair.

#### **Section 5.**

In the event a vacancy occurs in the office of the Chairperson, the Director shall designate a successor prior to the next regular or special meeting. In the event a vacancy occurs in the office of the Vice Chairperson, the membership of the Committee shall designate a successor at the next regular or special meeting (Penal Code 13810).

### **ARTICLE VII: QUORUM, VOTING AND ATTENDANCE**

#### **Section 1.**

A quorum of the Committee for any meeting shall consist of a majority of the members designated or appointed at the time of the meeting. If a quorum is present, a majority vote of the members present is necessary for Committee action, except for the suspension of these bylaws pursuant to Article XII.

#### **Section 2.**

No vote by an alternate will be honored except as provided for in this section.

- a) An alternate designation letter is required from any absent Committee member, and shall be presented to the Committee prior to the start of the next regular or special meeting.
- b) An alternate will have full voting rights, floor rights, and be included in quorum determinations.
- c) Alternated attendance for a Committee member will negate provision of Section 3 below.

#### **Section 3.**

Any member of the Committee who misses three consecutive meetings or who attends less than fifty percent of the Committee's regularly called meetings during one calendar year shall be automatically removed from the Committee, except in situations in which the Chair finds that such deficiency is the result of illness or injury.

## **ARTICLE VIII: REIMBURSEMENT OF EXPENSES**

### **Section 1.**

Members of the Committee shall not receive compensation for their services but will be reimbursed for those actual and necessary expenses incurred which relate to their duties as Committee members.

### **Section 2.**

Members of continuing task forces, review committees or of any other Committee-established auxiliary bodies who are not Committee members shall not receive compensation for expenses, unless prior approval has been obtained from the Office of Emergency Services. However, individuals who appear before the Committee at its request in order to review specific topics on one or more occasions shall be reimbursed for their necessary travel expenses.

## **ARTICLE IX: EXECUTIVE SECRETARY**

### **Section 1.**

The Executive Secretary of the Committee shall be appointed by the Director of the Office of Emergency Services

### **Section 2.**

The duties of the Executive Secretary to the Committee shall be to provide staff support to the Committee including keeping all records, preparing agendas for each meeting, keeping minutes and approving all Committee expenditures.

### **Section 3.**

The Executive Secretary shall, in accordance with applicable law, be responsible for any additional staffing, planning, organizing, coordinating, and directing to those activities necessary to assure the fulfillment of the powers, duties, and mission of the Committee.

## **ARTICLE X: CONFLICT OF INTEREST**

### **Section 1.**

No member of the Committee shall participate personally through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise in any proceeding, application, request for a ruling or other determination, contract, grant claim controversy, or other particular matter in which funds under jurisdiction of the Committee are used, where to his or her knowledge he or she or his or her immediate family, partners, organization other than a public agency in which he or she is serving is an officer, director, trustee, partner, or employee or any person or organization with who he or she is negotiating or has any arrangement concerning prospective employment, has a financial interest.

### **Section 2.**

In the review of proposals under appeal before the Committee, members of the Committee shall avoid any action which might result in, or create the appearance of:

- a) Using his or her official position for private gain;

- b) Giving preferential treatment to any person'
- c) Losing complete independence or impartiality;
- d) Making an official decision outside official channels; or
- e) Affecting adversely the confidence of the public in the integrity of the Government or the program.



## High Technology Theft Apprehension and Prosecution Program Area of Coverage

